Server Certificates Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

The need to communicate securely over public lines and the Internet resulted in the development of the Public Key Infrastructure (PKI) framework. PKI utilizes public-key cryptography and digital certificates to enable information to be sent in a secure and confidential manner.

# II. Purpose

Certificate Authorities (CA) sign and distribute certificates used to assure an identity when establishing encrypted communications. The purpose of this policy is to ensure proper controls are in place related to the selection of providers of trusted server-side third-party certificates and their implementation within ABC Company Information Resources.

# III. Scope

This policy applies to IT Department Staff responsible for administering and securing Information Resources.

# IV. Policy

Certificates are most commonly used for secure (https) Web sites. Web browsers inspect signed server-side certificates to verify that a Web server is authentic, using a specific Uniform Resource Locator (URL), and that the URL has been publicly verified with the identity of the institution. Using a server certificate helps assure the integrity and confidentiality of the encrypted communications through the use of cryptographic protocols such as Transport Layer Security (TLS).

Other types or classes of certificates may be installed on the client side web browser and used for the legal non-repudiation of transactions and multi-factor authentication, such as when the specific identity of individuals needs to be validated when connecting the server.

ABC Company’s IT Department shall ensure security controls protect sensitive communications by encrypting communication channels between endpoints using Transport Layer Security (TLS), or equivalent cryptographic protocols. Secure Hypertext Transport Protocol (HTTPS) connection based on server-side certificates shall be signed by a trusted third-party certificate provider.

To ensure that the security and integrity of the certificate remains intact, solutions must be installed and maintained according to the provider’s instructions and recommended use. Any deviation from the provider’s instructions or recommended use must be approved by the Director of IT and the Chief Security Officer.

Where possible, newer versions of TLS shall be used to protect authentication and communications against eavesdropping and tampering.

The use of wildcard certificates for one or more subdomains within the ABC Company domain is permissible under the following conditions:

* The service provided by the system may not be used to store or access sensitive data
* All requests for wildcard certificates are approved by the Director of IT prior to certificate purchase, acquisition or assignment.

Network administrators shall track certificate expiration dates to ensure that certificates are kept current and an expired certificate does not adversely impact business operations.

Self-signed certificates are only permitted for development systems that are segregated from the ABC Company production network and are not connected to external resources (e.g. Internet).

Network administrators shall comply with ABC Company’s Server Hardening Policy to ensure systems are protected from security and performance issues.

# V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to IT Department Staff responsible for administering and securing Information Resources.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO12.02, APO13.07, BAI02.05, BAI04.05, BAI05.09, BAI06.06, DSS04.07, MEA01.05

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.312(a)(2)(iv), 164.312(e)(2)(ii)

ISO 27001:2013 6.1.3, A.10, A.18.1.5

NIST SP 800-37 3.3, 3.4, 3.7

NIST SP 800-53 IA-7, SC-12, SC-13, SC-17

NIST Cybersecurity Framework ID.RA-6, PR.AC-3, DE.DP-2

PCI 2.1.1, 2.3, 3.4.1, 3.5-6, 4.1, 4.3, 6.5.3-4, 8.2.1